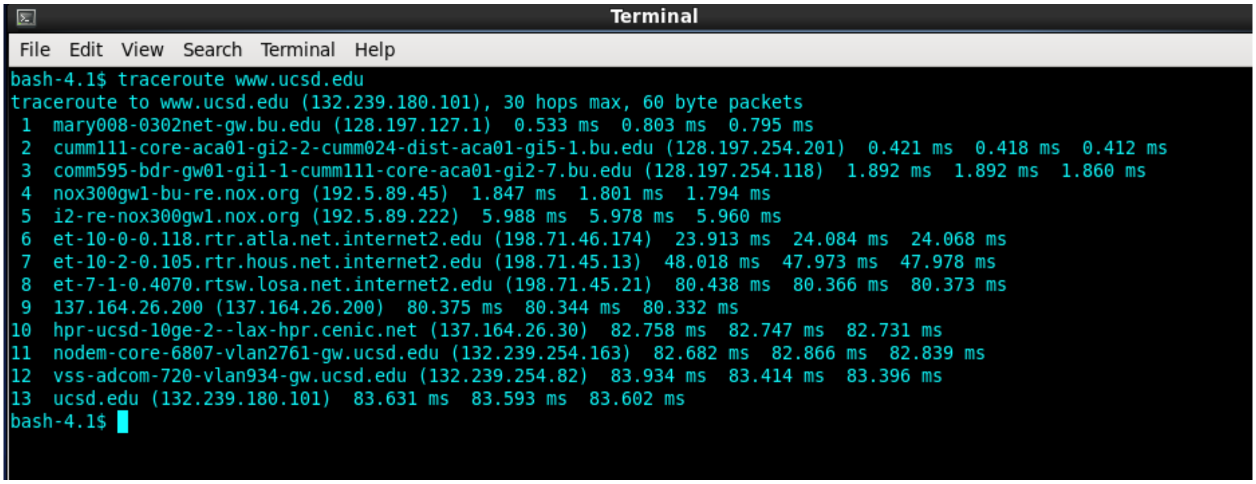
EC441: Lab 1

Daniel Andronov

Friday 23$^{\mathrm{rd}}$ September, 2016

1 Introduction to Traceroute



```
bash-4.1$ traceroute www.ucsd.edu
traceroute to www.ucsd.edu (132.239.180.101), 30 hops max, 60 byte packets
 1  mary008-0302net-gw.bu.edu (128.197.127.1)  0.533 ms  0.803 ms  0.795 ms
 2  cumm111-core-aca01-gi2-2-cumm024-dist-aca01-gi5-1.bu.edu (128.197.254.201)  0.421 ms  0.418 ms  0.412 ms
 3  comm595-bdr-gw01-gi1-1-cumm111-core-aca01-gi2-7.bu.edu (128.197.254.118)  1.892 ms  1.892 ms  1.860 ms
 4  nox300gw1-bu-re.nox.org (192.5.89.45)  1.847 ms  1.801 ms  1.794 ms
 5  i2-re-nox300gw1.nox.org (192.5.89.222)  5.988 ms  5.978 ms  5.960 ms
 6  et-10-0-0.118.rtr.atla.net.internet2.edu (198.71.46.174)  23.913 ms  24.084 ms  24.068 ms
 7  et-10-2-0.105.rtr.hous.net.internet2.edu (198.71.45.13)  48.018 ms  47.973 ms  47.978 ms
 8  et-7-1-0.4070.rtsw.losa.net.internet2.edu (198.71.45.21)  80.438 ms  80.366 ms  80.373 ms
 9  137.164.26.200 (137.164.26.200)  80.375 ms  80.344 ms  80.332 ms
10  hpr-ucsd-10ge-2--lax-hpr.cenic.net (137.164.26.30)  82.758 ms  82.747 ms  82.731 ms
11  nodem-core-6807-vlan2761-gw.ucsd.edu (132.239.254.163)  82.682 ms  82.866 ms  82.839 ms
12  vss-adcom-720-vlan934-gw.ucsd.edu (132.239.254.82)  83.934 ms  83.414 ms  83.396 ms
13  ucsd.edu (132.239.180.101)  83.631 ms  83.593 ms  83.602 ms
bash-4.1$ █
```

Question 1

Solution: 13 Hops.

Question 2

Solution: The traceroute seems to indicate that the packet traved through the ”altas” and ”cenic.net” ISP's.

Question 3

Solution: The locations of the routers involved in the traceroute are described in the following table

Hop No.	IP address	ISP	Location
1	128.197.127.1	Boston University	Boston, MA
2	128.197.254.201	Boston University	Boston, MA
3	128.197.254.118	Boston University	Boston, MA
4	192.5.89.45	Harvard University	Cambridge, MA
5	192.5.89.222	Harvard University	Cambridge, MA
6	198.71.46.174	Internet2	Ann Arbor, Michigan
7	198.71.45.13.	Internet2	Ann Arbor, Michigan
8	198.71.45.21	Internet2	Ann Arbor, Michigan
9	137.164.26.200	CENIC	Cypress, California
10	137.164.26.30	CENIC	Cypress, California
11	132.239.254.163	UCSD	La Jolla, California
12	132.239.254.82	UCSD	La Jolla, California
13	132.239.180.101	UCSD	La Jolla, California

Question 4

Solution: traceroute www.ucsd.ed -N 10

Question 5

Solution: The round trip time to the destination was occasionally faster that the intermediate. This is most probably due to some traffic on the route to the destination or that the packet took some longer route that is not shown in the traceroute output.

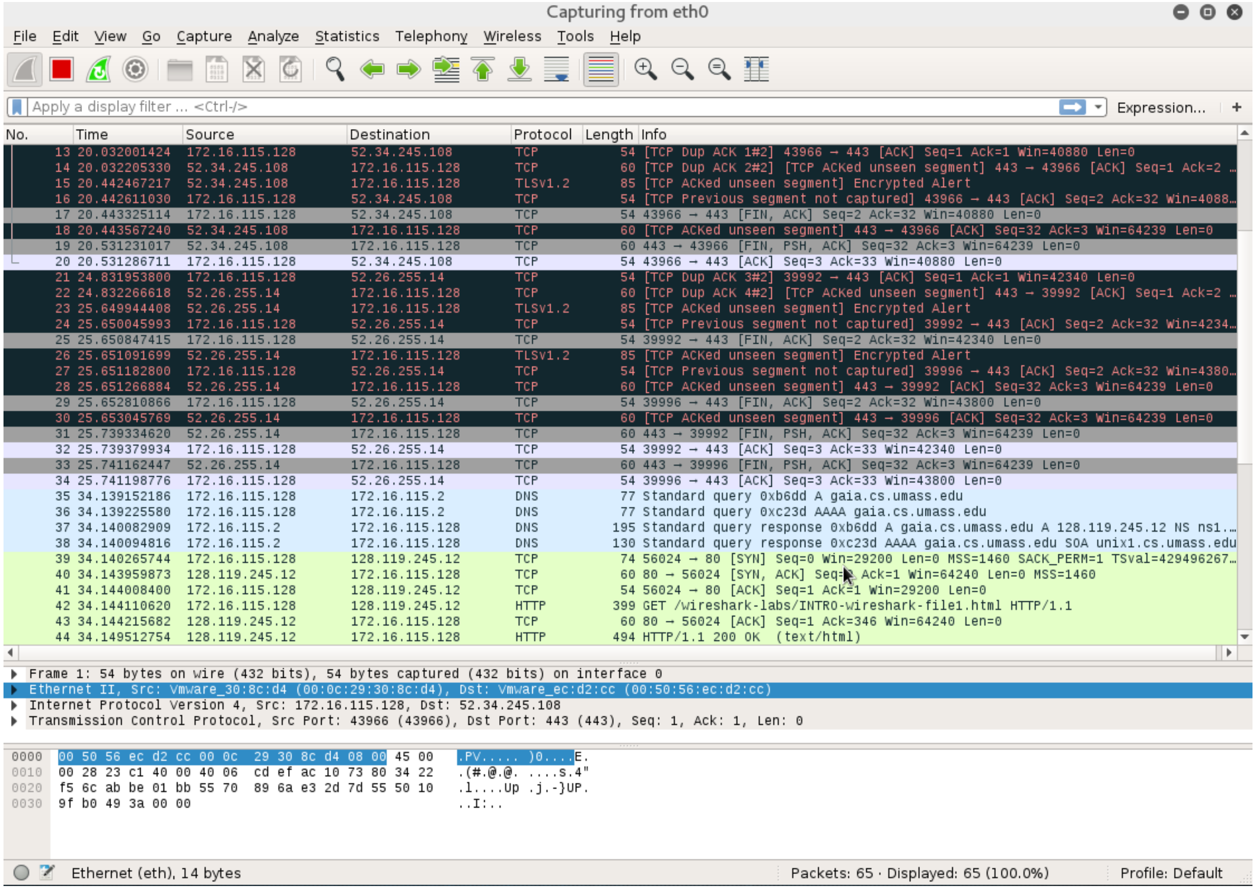
Question 6

Solution:

Trial No.	Probe 1 RRT	Probe 2 RRT	Probe 3 RRT
1	83.526	83.511	83.423
2	83.631	83.593	83.602
3	85.565	83.596	84.265
4	83.494	83.391	83.906

The RTT to the destiniation has average 83.792 ms and standard devation 0.581 ms.

2 Wireshark Experiments


Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
+

```
No.  Time          Source          Destination     Protocol Length Info
  13 20.032001424  172.16.115.128  52.34.245.108   TCP        54 [TCP Dup ACK 1#2] 43966 → 443 [ACK] Seq=1 Ack=1 Win=40880 Len=0
  14 20.032205330  52.34.245.108   172.16.115.128  TCP        60 [TCP Dup ACK 2#2] [TCP ACKed unseen segment] 443 → 43966 [ACK] Seq=1 Ack=2 …
  15 20.442467217  52.34.245.108   172.16.115.128  TLSv1.2    85 [TCP ACKed unseen segment] Encrypted Alert
  16 20.442611030  172.16.115.128  52.34.245.108   TCP        54 [TCP Previous segment not captured] 43966 → 443 [ACK] Seq=2 Ack=32 Win=4088…
  17 20.443325114  172.16.115.128  52.34.245.108   TCP        54 43966 → 443 [FIN, ACK] Seq=2 Ack=32 Win=40880 Len=0
  18 20.443567240  52.34.245.108   172.16.115.128  TCP        60 [TCP ACKed unseen segment] 443 → 43966 [ACK] Seq=32 Ack=3 Win=64239 Len=0
  19 20.531231017  52.34.245.108   172.16.115.128  TCP        60 443 → 43966 [FIN, PSH, ACK] Seq=32 Ack=3 Win=64239 Len=0
  20 20.531286711  172.16.115.128  52.34.245.108   TCP        54 43966 → 443 [ACK] Seq=3 Ack=33 Win=40880 Len=0
  21 24.831953800  172.16.115.128  52.26.255.14    TCP        54 [TCP Dup ACK 3#2] 39992 → 443 [ACK] Seq=1 Ack=1 Win=42340 Len=0
  22 24.832266618  52.26.255.14    172.16.115.128  TCP        60 [TCP Dup ACK 4#2] [TCP ACKed unseen segment] 443 → 39992 [ACK] Seq=1 Ack=2 …
  23 25.649944408  52.26.255.14    172.16.115.128  TLSv1.2    85 [TCP ACKed unseen segment] Encrypted Alert
  24 25.650045993  172.16.115.128  52.26.255.14    TCP        54 [TCP Previous segment not captured] 39992 → 443 [ACK] Seq=2 Ack=32 Win=4234…
  25 25.650847415  172.16.115.128  52.26.255.14    TCP        54 39992 → 443 [FIN, ACK] Seq=2 Ack=32 Win=42340 Len=0
  26 25.651091699  52.26.255.14    172.16.115.128  TLSv1.2    85 [TCP ACKed unseen segment] Encrypted Alert
  27 25.651182800  172.16.115.128  52.26.255.14    TCP        54 [TCP Previous segment not captured] 39996 → 443 [ACK] Seq=2 Ack=32 Win=4380…
  28 25.651266884  52.26.255.14    172.16.115.128  TCP        60 [TCP ACKed unseen segment] 443 → 39992 [ACK] Seq=32 Ack=3 Win=64239 Len=0
  29 25.652810866  172.16.115.128  52.26.255.14    TCP        54 39996 → 443 [FIN, ACK] Seq=2 Ack=32 Win=43800 Len=0
  30 25.653045769  52.26.255.14    172.16.115.128  TCP        60 [TCP ACKed unseen segment] 443 → 39996 [ACK] Seq=32 Ack=3 Win=64239 Len=0
  31 25.739334620  52.26.255.14    172.16.115.128  TCP        60 443 → 39992 [FIN, PSH, ACK] Seq=32 Ack=3 Win=64239 Len=0
  32 25.739379934  172.16.115.128  52.26.255.14    TCP        54 39992 → 443 [ACK] Seq=3 Ack=33 Win=42340 Len=0
  33 25.741162447  52.26.255.14    172.16.115.128  TCP        60 443 → 39996 [FIN, PSH, ACK] Seq=32 Ack=3 Win=64239 Len=0
  34 25.741198776  172.16.115.128  52.26.255.14    TCP        54 39996 → 443 [ACK] Seq=3 Ack=33 Win=43800 Len=0
  35 34.139152186  172.16.115.128  172.16.115.2    DNS        77 Standard query 0xb6dd A gaia.cs.umass.edu
  36 34.139225580  172.16.115.128  172.16.115.2    DNS        77 Standard query 0xc23d AAAA gaia.cs.umass.edu
  37 34.140082909  172.16.115.2    172.16.115.128  DNS       195 Standard query response 0xb6dd A gaia.cs.umass.edu A 128.119.245.12 NS ns1.…
  38 34.140094816  172.16.115.2    172.16.115.128  DNS       130 Standard query response 0xc23d AAAA gaia.cs.umass.edu SOA unix1.cs.umass.edu
  39 34.140265744  172.16.115.128  128.119.245.12  TCP        74 56024 → 80 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM=1 TSval=429496267…
  40 34.143959873  128.119.245.12  172.16.115.128  TCP        60 80 → 56024 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
  41 34.144008400  172.16.115.128  128.119.245.12  TCP        54 56024 → 80 [ACK] Seq=1 Ack=1 Win=29200 Len=0
  42 34.144110620  172.16.115.128  128.119.245.12  HTTP      399 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
  43 34.144215682  128.119.245.12  172.16.115.128  TCP        60 80 → 56024 [ACK] Seq=1 Ack=346 Win=64240 Len=0
  44 34.149512754  128.119.245.12  172.16.115.128  HTTP      494 HTTP/1.1 200 OK  (text/html)
```

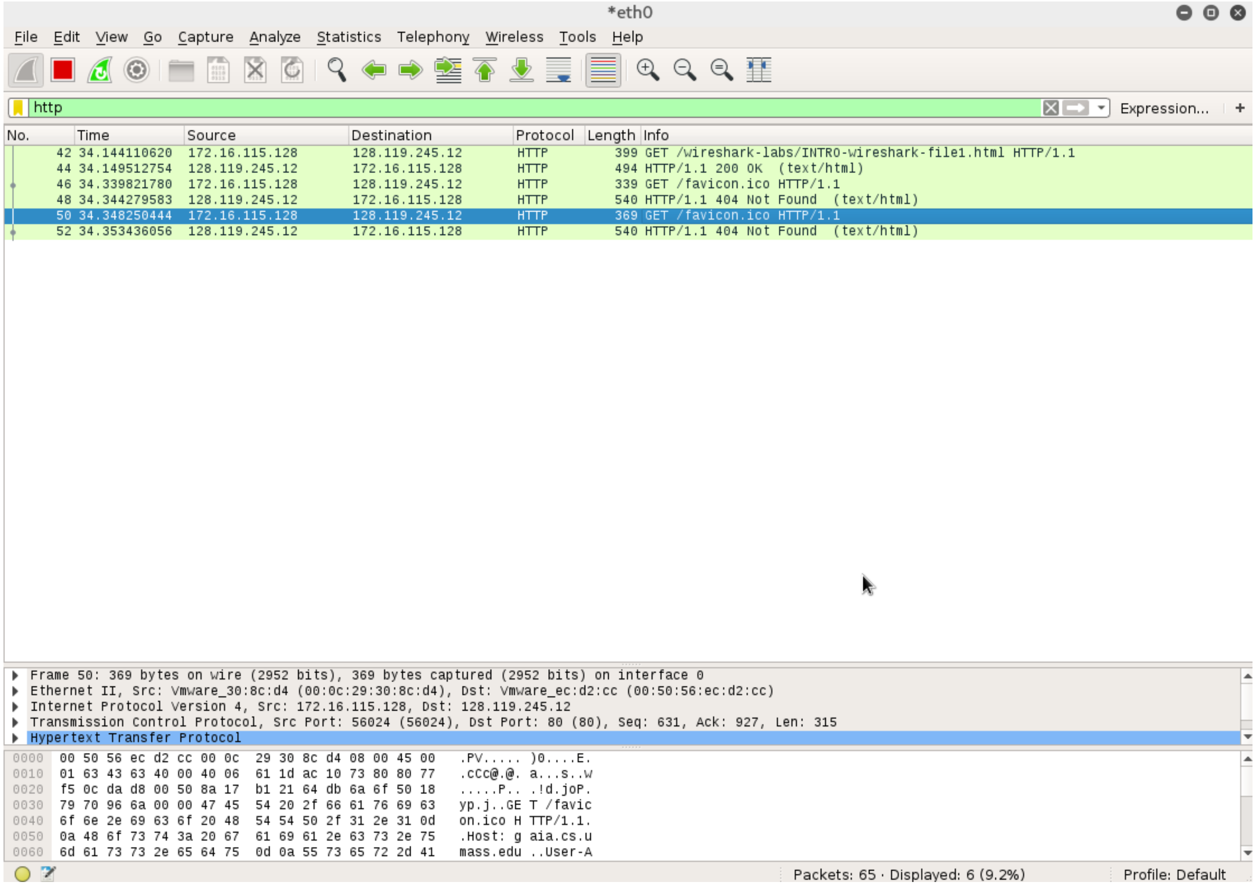
```
▶ Frame 1: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
▶ Ethernet II, Src: Vmware_30:8c:d4 (00:0c:29:30:8c:d4), Dst: Vmware_ec:d2:cc (00:50:56:ec:d2:cc)
▶ Internet Protocol Version 4, Src: 172.16.115.128, Dst: 52.34.245.108
▶ Transmission Control Protocol, Src Port: 43966 (43966), Dst Port: 443 (443), Seq: 1, Ack: 1, Len: 0
```

```
0000  00 50 56 ec d2 cc 00 0c  29 30 8c d4 08 00 45 00   .PV..... )0....E.
0010  00 28 23 c1 40 00 40 06  cd ef ac 10 73 80 34 22   .(#.@.@. ....s.4"
0020  f5 6c ab be 01 bb 55 70  89 6a e3 2d 7d 55 50 10   .l....Up .j.-}UP.
0030  9f b0 49 3a 00 00                                  ..I:..
```

Ethernet (eth), 14 bytes   Packets: 65 · Displayed: 65 (100.0%)   Profile: Default

Question 7

Solution: TCP, HTTP TLSv1.2


*eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
http
Expression...
+

```
No.   Time         Source           Destination      Protocol Length Info
   42 34.144110620 172.16.115.128   128.119.245.12   HTTP      399 GET /wireshark-labs/INTRO-wireshark-file1.html HTTP/1.1
   44 34.149512754 128.119.245.12   172.16.115.128   HTTP      494 HTTP/1.1 200 OK  (text/html)
   46 34.339821780 172.16.115.128   128.119.245.12   HTTP      339 GET /favicon.ico HTTP/1.1
   48 34.344279583 128.119.245.12   172.16.115.128   HTTP      540 HTTP/1.1 404 Not Found  (text/html)
   50 34.348250444 172.16.115.128   128.119.245.12   HTTP      369 GET /favicon.ico HTTP/1.1
   52 34.353436056 128.119.245.12   172.16.115.128   HTTP      540 HTTP/1.1 404 Not Found  (text/html)
```

```
▶ Frame 50: 369 bytes on wire (2952 bits), 369 bytes captured (2952 bits) on interface 0
▶ Ethernet II, Src: Vmware_30:8c:d4 (00:0c:29:30:8c:d4), Dst: Vmware_ec:d2:cc (00:50:56:ec:d2:cc)
▶ Internet Protocol Version 4, Src: 172.16.115.128, Dst: 128.119.245.12
▶ Transmission Control Protocol, Src Port: 56024 (56024), Dst Port: 80 (80), Seq: 631, Ack: 927, Len: 315
▶ Hypertext Transfer Protocol
```

```
0000  00 50 56 ec d2 cc 00 0c  29 30 8c d4 08 00 45 00   .PV..... )0....E.
0010  01 63 43 63 40 00 40 06  61 1d ac 10 73 80 80 77   .cCc@.@. a...s..w
0020  f5 0c da d8 00 50 8a 17  b1 21 64 db 6a 6f 50 18   .....P.. .!d.joP.
0030  79 70 96 6a 00 00 47 45  54 20 2f 66 61 76 69 63   yp.j..GE T /favic
0040  6f 6e 2e 69 63 6f 20 48  54 54 50 2f 31 2e 31 0d   on.ico H TTP/1.1.
0050  0a 48 6f 73 74 3a 20 67  61 69 61 2e 63 73 2e 75   .Host: g aia.cs.u
0060  6d 61 73 73 2e 65 64 75  0d 0a 55 73 65 72 2d 41   mass.edu ..User-A
```

Packets: 65 · Displayed: 6 (9.2%) Profile: Default

Question 8 Solution: The GET packet was timestamped at 34.144110620 and the OK packet was timestamped at 34.149512754 sec, so the time in between the two packets was 0.005402134 sec or about 5.4 ms.

Question 9
Solution: 128.119.245.12

Question 10
Solution: 172.16.115.128

Question 11
Solution: The IP addresses starting with 192.168.x.x and 172.16.x.x are two of three sets of IP adresses reserved for private netorks, with the last reserved address is 10.x.x.x. These three addresses ranges are called classes, with each having more addresses to support connected devices than the last. They are ordered as below.

Address Range	Class Type	Maximum Devices
192.168.x.x	A	65,536
172.16.x.x - 172.31.x.x	B	1,048,576
10.x.x.x	C	16,777,216